

## CLAIMS

What is claimed is:

- Sub  
a1
- 1 1. A method comprising:  
2 providing a key matrix having N rows and M columns of matrix keys, where  $N \geq 2$  and  
3  $M \geq 2$ ;  
4 for each column of the key matrix, performing arithmetic operations on matrix keys  
5 of at least two selected rows of the key matrix to produce a first set of secret device keys;  
6 producing a shared secret key based on arithmetic operations on selected secret device  
7 keys of the first set of secret device keys.
- 1 2. The method of claim 1, wherein the arithmetic operations include modular  
2 addition.
- 1 3. The method of claim 1, wherein prior to performing the arithmetic operations,  
2 the method comprises:  
3 generating a key selection vector identifying the at least two selected rows of the key  
4 matrix from which to produce the first set of secret device keys.
- 1 4. The method of claim 3, wherein the key selection vector is uniquely assigned  
2 to a first digital platform.
- 1 5. The method of claim 4, wherein prior to producing the shared secret key, the  
2 method comprises:  
3 receiving a key selection vector from a second digital platform in communication  
4 with the first digital platform; and

5 analyzing contents of the key selection vector from the second digital platform to  
6 determine the selected secret device keys of the first set of secret device keys.

1 6. The method of claim 1, wherein prior to performing arithmetic operations on  
2 keys of at least two selected rows, the method further comprises:  
3 dedicating the rows of the key matrix to a first classification; and  
4 dedicating the columns of the key matrix to a second classification.

1 7. The method of claim 6, wherein the first classification includes digital  
2 platforms designed to provide information to other digital platforms.

1 8. The method of claim 7, wherein the second classification includes digital  
2 platforms designed to receive information from other digital platforms.

1 9. The method of claim 1, wherein the producing of the shared secret key  
2 comprises:  
3 analyzing contents of an incoming key selection vector; and  
4 performing arithmetic operations of the selected secret device keys located in  
5 columns of the key matrix identified by the contents of the incoming key selection vector.

1 10. The method of claim 9, wherein the producing of the shared secret key further  
2 comprises:  
3 performing a hash operation on results of the arithmetic operations of the selected  
4 secret device keys located in the column of the key matrix identified by the contents of the  
5 incoming key selection vector.

1 11. A method comprising:

2 providing a key matrix having N rows and M columns of matrix keys, where  $N \geq 2$  and  
3  $M \geq 2$ ;  
4 for each row of the key matrix, performing arithmetic operations on matrix keys of at  
5 least two selected columns of the key matrix to produce a first set of secret device keys;  
6 producing a shared secret key based on arithmetic operations on selected secret device  
7 keys of the first set of secret device keys.

1 12. The method of claim 11, wherein the arithmetic operations include modular  
2 addition.

1 13. The method of claim 11, wherein prior to performing the arithmetic  
2 operations, the method comprises:  
3 generating a key selection vector identifying the at least two selected rows of the key  
4 matrix from which to produce the first set of secret device keys.

1 14. The method of claim 13, wherein the key selection vector is uniquely assigned  
2 to a first digital platform.

1 15. The method of claim 14, wherein prior to producing the shared secret key, the  
2 method comprises:  
3 receiving a key selection vector from a second digital platform in communication  
4 with the first digital platform; and  
5 analyzing contents of the key selection vector from the second digital platform to  
6 determine the selected secret device keys of the first set of secret device keys.

1 16. The method of claim 1, wherein prior to performing arithmetic operations on  
2 keys of at least two selected columns, the method further comprises:



1           20.     A network comprising:  
2           a first digital platform; and  
3           a certification authority in communication with the first digital platform, the  
4     certification authority having access to a key matrix featuring matrix keys arranged in  
5     accordance with at least a first dimension and a second dimension, generating a first key  
6     selection vector and providing a first set of secret device keys produced from selected matrix  
7     keys of the key matrix.

1           21.     The network of claim 20 further comprising:  
2           a second digital platform in communication with the certification authority and the  
3     first digital platform, the second digital platform being uniquely assigned a second key  
4     selection vector indicating at least two grids of the key matrix and a second set of secret  
5     device keys produced from matrix keys situated in at least two grids of the key matrix.

1           22.     The network of claim 21, wherein the first and second digital platforms to  
2     exchange the first and second key selection vectors in order for each digital platform to  
3     produce a shared secret key to ensure that communications between the first and second  
4     digital platforms are secure.

1           23.     A certification authority comprising:  
2           a memory to store a key matrix having N rows and M columns of matrix keys, where  
3      $N \geq 2$  and  $M \geq 2$ ;  
4           a logic to generate a key selection vector for each digital platform registered with the  
5     certification authority.

0042390"22752260

1           24.    The certification authority of claim 23, wherein the logic includes a processing  
2   unit.

1           25.    The certification authority of claim 24, wherein the processing unit produces a  
2   first set of secret device keys by performing arithmetic operations on matrix keys along  
3   selected columns of the key matrix identified by the key selection vector to provide a first set  
4   of secret device keys to a digital platform.

1           26.    The certification authority of claim 25, wherein the matrix keys along the  
2   processing unit performs arithmetic operations on matrix keys along selected rows of the key  
3   matrix identified by the key selection vector to provide a first set of secret device keys to a  
4   digital platform.

1           27.    The certification authority of claim 23, wherein the matrix keys are only  
2   known by the certification authority.